REMARKS

Applicant has carefully reviewed the Final Office Action mailed February 2, 2007 and offers the following remarks to accompany the above amendments.

Claim 1 has been amended to add the limitations of dependent claims 2, 4, and 7 and to remove the cleansing limitation from the independent claim. The cleansing limitation is now found in new dependent claim 27. Claims 2, 4, and 7 have been cancelled accordingly. Claim 17 has been amended to include the limitations of claims 18 and 19 and to remove the cleaning limitation from the independent claim. The cleaning limitation is now found in new dependent claim 29. Claims 18 and 19 are thus cancelled. Claims 13-16, 22, and 23 have also been cancelled. Claims 3 and 26 have been amended to correct their dependency. New claims 27-31 have been added. No new matter has been added as a result of these claim amendments.

Claims 1-7, 9-11, 13-20, and 22-26 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,529,992 B1 to Thomas et al. (hereinafter "Thomas") in view of U.S. Patent No. 6,055,314 to Spies et al. (hereinafter "Spies"). Applicant respectfully traverses. To establish *prima facie* obviousness, each and every element of the claim must be taught or suggested in the combination of references. MPEP § 2143.03.

Before addressing the rejections, Applicant provides a brief overview of the invention as background. The present invention relates to a portable device configured to interact with any number of host computing devices. In operation, the portable device will initially appear to a host computing device as a known device type, such as a storage device. The host computing device will be configured to interact with the portable device as the storage device. Upon such interaction, the host computing device will access indicia sufficient to identify the portable device as a second device type, such as a cryptographic service provider, and instruct the host computing device to configure itself to interact with the portable device as the cryptographic service provider. Notably, in one embodiment, portable devices equipped with processing capabilities may operate to provide processing for the services provided by the cryptographic service provider on the portable device. In particular, the portable device may include a processing unit associated with the memory of the portable device that is used to provide the cryptography services to the host computing device, such that the portable device operates as a hardware-based cryptographic service provider.

Claim 1 as amended recites a portable device for engaging a host computing device comprising:

a body;

a memory within the body containing:

initial identification indicia to initially identify the portable device to the host computing device as a storage device, which is known to the host computing device;

configuration indicia to subsequently identify the portable device to the host computing device as a cryptographic service provider and provide configuration instructions to allow the host computing device to effectively interact with the portable device as the cryptographic service provider;

service indicia providing instructions to provide a service corresponding to the cryptographic service provider; and

an interface associated with the memory and adapted to facilitate interaction with the host computing device; and

a processing unit associated with the memory, wherein the service indicia includes instructions for the processing unit to provide the service corresponding to the cryptographic service provider to the host computing device.

Thus, the single portable device of the present invention can operate as both a known storage device and as a cryptographic service provider. In amended claim 1 (and new dependent method claim 29)[1], the portable device also includes a processing unit of the portable device, which is used to provide the cryptography service to the host computing device. As such, the portable device is initially identified as a known storage device to the host, and then runs configuration software from the portable device on the host device in order that the portable device can serve as a cryptographic service provider. In this way, the portable device is a true two-in-one device that performs both as a storage device and a cryptographic service provider. Neither Thomas nor Spies teaches or suggests such a two-in-one portable device that operates both as a storage device and as a cryptographic service provider. In addition, neither Thomas nor Spies teaches or suggests where the portable device includes a processing unit associated with said memory, wherein the service indicia includes instructions for said processing unit to provide

[1] New dependent claim 29 includes a processing unit limitation similar to amended claim 1, and thus is patentable for at least the same reasons as claim 1.

the service corresponding to the cryptographic service provider for the host computing device, as recited in claim 1. That is, neither Thomas nor Spies teaches or suggests a portable device that operates as a hardware-based cryptographic service provider. Therefore, the combination of Thomas and Spies does not teach each and every limitation of claim 1. Accordingly, claim 1 is patentable.

The Patent Office asserts that Thomas at col. 5, lines 25-44 teaches wherein the first device type is a storage device (Final Office Action mailed February 2, 2007, p. 8). Thomas does disclose a media drive, such as a ZIP drive. However, Thomas does not teach or suggest a portable device having a memory within the body that contains initial identification indicia to initially identify the portable device to the host computing device as a storage device, configuration indicia to subsequently identify the portable device to the host computing device as a cryptographic service provider and provide configuration instructions to allow the host computing device to effectively interact with the portable device as the cryptographic service provider, and service indicia providing instructions to provide a service corresponding to the cryptographic service provider to the host computing device, as claimed by the present invention. Although Thomas may disclose a ZIP drive, it does not teach or suggest a portable device that is initially identified to the host device as a storage device and then configured to act as a cryptographic service provider that provides cryptography services to the host. Spies likewise does not teach such a portable device. Thus, the combination of Thomas and Spies does not teach each and every limitation of claim 1. Accordingly, claim 1 is patentable.

In addition, neither Thomas nor Spies teaches or suggests where the portable device includes a processing unit associated with said memory, wherein the service indicia includes instructions for said processing unit to provide the service corresponding to the cryptographic service provider for the host computing device. That is, neither Thomas nor Spies teaches or suggests a portable device that operates as a hardware-based cryptographic service provider. The Patent Office asserts that Thomas, as modified by Spies, teaches a processing unit associated with the memory and wherein the service indicia includes instructions for the processing unit to provide the cryptography services for the host computing device, and cites to Thomas, Figure 2, ref. num. 106 as being the claimed processing unit (Final Office Action mailed February 2, 2007, p. 7). Element 106 of Figure 2 in Thomas is a microcontroller within the PHAEDRUS 105. There is no mention in Thomas of what the microcontroller 106 actually does. Certainly, there is

no teaching or suggestion that the microcontroller 106 of Thomas provides cryptography services for the host computing device. Thus, it is clear that the microcontroller 106 of Thomas cannot be the claimed processing unit that provides the cryptography service to the host computing device. Since Thomas, either alone or in combination with Spies, does not teach or suggest each and every element of the claimed invention, the claimed invention is patentable.

Claim 17 contains limitations similar to those in claim 1, and is patentable for at least the same reasons set forth above with respect to claim 1. However, claim 17 is slightly different from claim 1. Claim 17 includes the limitations "identifying a portable device to a host computing device as a storage device, which is known to the host computing device"; "registering the portable device with the host computing device as the storage device"; "automatically identifying the portable device to the host computing device as a cryptographic service provider"; and "enabling the portable device as the cryptographic service provider with the host computing device based on information provided on the portable device." As discussed above, the combination of Thomas and Spies fails to teach or suggest where a portable device is identified to the host computing device as a portable device and then is subsequently identified as a cryptographic service provider. In addition, neither Thomas nor Spies, either alone or in combination, teaches or suggests where the identifying the portable device as a cryptographic service provider is **automatic**. The Patent Office cites to Figure 6, element 104, to col. 11, line 64 through col. 12, line 1, and to col. 12, lines 41-44 of Spies as allegedly teaching "automatically identifying the portable device to the host computing device as a cryptographic service provider" (Final Office Action mailed February 6, 2007, p. 6). Applicant has reviewed the cited portions of Spies. First of all, although Spies does disclose an IC card that when coupled to a viewer computing unit, cooperates to form a video decryption device; there is no mention of identifying the IC card as two different device types (first a storage device and then a cryptographic service provider). In addition, there is no teaching or suggestion that the IC card is **automatically** identified as a cryptographic service provider after being first identified and registered as a storage device, as required by claim 17. Thus, for at least these reasons, claim 17 is patentable.

Claims 3, 5, 6, 9-11, and 24-26 depend from claim 1 and contain all the limitations of claim 1. Therefore, claims 3, 5, 6, 9-11, and 24-26 are patentable for at least the same reasons as set forth above with respect to claim 1. Claim 20 depends from claim 17 and contains all the

limitations of claim 17. Therefore, claim 20 is patentable for at least the same reasons as set forth above with respect to claim 17.

In particular, claim 5 recites that the configuration indicia includes a file executable on the host computing device to reconfigure the host computing device to recognize and interact with the portable device as the cryptographic service provider. Dependent claim 30 has a similar limitation. Neither Thomas nor Spies, either alone or in combination, teaches or suggests such a limitation. The Patent Office refers to Thomas, Figure 4, and Spies, Figure 6, ref. num. 118 as allegedly teaching this limitation (Final Office Action mailed February 2, 2007, p. 8). Applicant respectfully traverses. Figure 4 of Thomas is a task disk control file. This file does contain configuration instructions. However, the task disk control file of Thomas does not execute on the host computing device to reconfigure the host computing device to recognize and interact with the portable device as the cryptographic service provider. Likewise, ref. num. 118 in Figure 6 of Spies refers to RSA encryption algorithms. These algorithms are the encryption algorithms themselves; they are not configuration indicia on the portable device that are executable on the host computing device to reconfigure the host computing device to recognize and interact with the portable device as the cryptographic service provider. Accordingly, neither Thomas nor Spies, either alone or in combination, teaches or suggests a portable device "wherein the configuration indicia includes a file executable on the host computing device to reconfigure the host computing device to recognize and interact with the portable device as the cryptographic service provider," as recited in claim 5. Therefore, claim 5 and claim 30, which contains a similar limitation, are separately patentable for this additional reason.

The present application is now in condition for allowance and such action is respectfully requested. The Examiner is encouraged to contact Applicant's representative regarding any remaining issues in an effort to expedite allowance and issuance of the present application.

Respectfully submitted,

WITHROW & TERRANOVA, P.L.L.C.

By: John R. Witcher, III

John R. Witcher, III
Registration No. 39,877
100 Regency Forest Drive, Suite 160
Cary, NC 27518
Telephone: (919) 238-2300

Date: May 1, 2007
Attorney Docket: 4989-009